THAT WHICH IS CLAIMED:

1. A method for generating a key for data encryption in a communication network, the method comprising the steps of:

selecting a first secret key;

combining the first secret key with at least a portion of a user-specific Medium Access Control (MAC) address to result in an intermediate value; and

combining the intermediate value with predefined key change information

2. The method of Claim 1, further comprising transforming the combination of the intermediate value and the predefined key change information to generate the key.

3. The method of Claim 2 wherein transforming comprises hashing the combination of the intermediate value and the predefined key change information to generate the key.

4. The method of Claim 1, wherein selecting a first secret key further comprises selecting one of several predefined secret keys.

5. The method of Claim 1, wherein combining the first secret key with a user-specific MAC address further comprises performing a bitwise exclusive OR (XOR) operation.

6. The method of Claim 1 further comprising obtaining the predefined key change information from a MAC data packet.

7. The method of Claim 1, wherein combining the second secret key with the predefined key change information further comprises performing a bitwise XOR operation.

8. A method for generating a key for data encryption in a communication network, the method comprising the steps of:

generating an Initialization Vector (IV) value;

combining a first secret key with the IV value to result in an intermediate value; and

permutating the intermediate value.

9. The method of Claim 8, further comprising computing the first secret key by selecting a predetermined secret key, combining the predetermined secret key with a user-specific Medium Access Control (MAC) address to result in a first intermediate value, combining the intermediate value with predefined key change information and transforming the combination of the intermediate value and the predefined key change information to result in the first secret key.

10. The method of Claim 8, wherein generating an Initialization Vector (IV) value further comprises the steps of:

concatenating a timer value and at least a portion of a MAC address to result in a seed value; and

applying the seed value to a random number generator to result in the IV value.

11. The method of Claim 8, wherein combining the first secret key with the IV value further comprises performing a bitwise exclusive OR (XOR) operation.

12. A method for generating a key for data encryption in a communication network, the method comprising the steps of:

calculating a first secret key utilizing predefined key change information;

determining if the key change information has repeated; and

differently processing the first secret key to generate the key for data encryption in instances in which the key change information has repeated than in instances in which the key change information has not repeated.

13. A method according to Claim 12 wherein differently processing the first secret key comprises performing a bitwise shift of the first secret key in instances in which the key change information has not repeated.

14. The method of Claim 11 wherein calculating a first secret key further comprises the steps of selecting a predetermined secret key, combining the predetermined secret key with a user-specific Medium Access Control (MAC) address to result in a first intermediate value, combining the first intermediate value with predefined key change information, transforming the combination of the intermediate value and the predefined key change information to result in a temporary key, combining the temporary key and an IV value and permutating the combination of the temporary key and the IV value to result in the first secret key.

15. A method for generating a key for data encryption in a communication network, the method comprising the steps of:

selecting a first secret key;

generating a first temporary key based upon a combination of the first secret key with at least a portion of a user-specific Medium Access Control (MAC) address and further based upon predefined key change information;

generating a second temporary key based upon a combination of the first temporary key and an Initialization Vector (IV) value;

determining if the predefined key change information has repeated; and

generating the key for data encryption based upon the second temporary key and the determination if the predefined key change information has repeated.

16. The method of Claim 15, wherein generating the key for data encryption comprises differently processing the second temporary key to generate the key for data encryption in instances in which the key change information has repeated than in instances in which the key change information has not repeated.

17. A method according to Claim 16 wherein differently processing the second temporary key comprises performing a bitwise shift of the second temporary key in instances in which the key change information has not repeated.

18. The method of Claim 15, wherein generating the first temporary key further comprises combining an intermediate value generated by the combination of the first secret key with at least a portion of the user-specific MAC address with the predefined key change information and thereafter transforming the combination of the intermediate value and the predefined key change information to generate the first temporary key.

19. The method of Claim 18 wherein transforming comprises hashing the combination of the intermediate value and the predefined key change information to generate the first temporary key.

20. The method of Claim 15, wherein generating the second temporary key comprises permutating the combination o the first temporary key and the IV value.

21. The method of Claim 15, wherein generating the second temporary key comprises generating the IV value by concatenating a timer value and at least a portion of a MAC address to result in a seed value and applying the seed value to a random number generator to result in the IV value.

22. A method for data encryption in a communication network, the method comprising the steps of:

generating a first temporary key based upon a combination of a first secret key with at least a portion of a user-specific Medium Access Control (MAC) address and further based upon predefined key change information;

generating a second temporary key based upon a combination of the first temporary key and an Initialization Vector (IV) value;

determining if the predefined key change information has repeated;

generating a final key based upon the second temporary key and the determination if the predefined key change information has repeated; and

encrypting data transmitted via the communication network with the final key.

23. A method according to Claim 22 further comprising:

determining if the data is originally encrypted in accordance with a predetermined encryption technique; and

decrypting the data if the data is originally encrypted in accordance with the predetermined encryption technique, prior to encrypting the data transmitted via the communication network with the final key.

24. A method according to Claim 24 wherein determining if the data is originally encrypted comprises determining if the data is originally encrypted in accordance with a WEP technique.

25. A computer program product readable by a machine and tangibly embodying a program of instructions executable by the machine to perform steps for data encryption, the program of instructions comprising the steps of:

generating a first temporary key based upon a combination of a first secret key with at least a portion of a user-specific Medium Access Control (MAC) address and further based upon predefined key change information;

generating a second temporary key based upon a combination of the first temporary key and an Initialization Vector (IV) value;

determining if the predefined key change information has repeated;

generating a final key based upon the second temporary key and the determination if the predefined key change information has repeated; and

encrypting data transmitted via the communication network with the final key.

26. The computer program product of Claim 25 wherein the program of instructions further comprises the steps of:

determining if the data is originally encrypted in accordance with a predetermined encryption technique; and

decrypting the data if the data is originally encrypted in accordance with the predetermined encryption technique, prior to encrypting the data transmitted via the communication network with the final key.

27. The computer program product of Claim 25, wherein the step of generating the key for data encryption comprises differently processing the second temporary key to generate the key for data encryption in instances in which the key change information has repeated than in instances in which the key change information has not repeated.

28. The computer program product of Claim 16 wherein the step of differently processing the second temporary key comprises performing a

bitwise shift of the second temporary key in instances in which the key change information has not repeated.

29. The computer program product of Claim 25 wherein the step of generating the first temporary key further comprises combining an intermediate value generated by the combination of the first secret key with at least a portion of the user-specific MAC address with the predefined key change information and thereafter transforming the combination of the intermediate value and the predefined key change information to generate the first temporary key.

30. The computer program product of Claim 29 wherein transforming comprises hashing the combination of the intermediate value and the predefined key change information to generate the first temporary key.

31. The computer program product of Claim 25, wherein the step of generating the second temporary key comprises permutating the combination o the first temporary key and the IV value.

32. The computer program product of Claim 25, wherein the step of generating the second temporary key comprises generating the IV value by concatenating a timer value and at least a portion of a MAC address to result in a seed value and applying the seed value to a random number generator to result in the IV value.